FEASIBILITY REPORT

REPORT FOR THE CONGRESS OF THE UNITED STATES MARCH 2008

Prepared by the
Program Manager, Information Sharing Environment

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Feasibility Report: Report for the Congress of the United States	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Director of National Intelligence,Program Manager,Information Sharing Environment,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**23**	

Table of Contents

1. Introduction

1.1. 9/11 Act Requirements

In the recently enacted "Implementing Recommendations of the 9/11 Commission Act of 2007 (the "9/11 Act"), Congress requested that the President report on the feasibility of the following, with respect to the Information Sharing Environment (ISE):

- *Eliminating the use of any marking or process (including 'Originator Control') intended to, or having the effect of, restricting the sharing of information within the scope of the ISE unless the President has specifically exempted categories of information from such elimination; and*
- *Continuing to use Federal agency standards for the collection, sharing, and access to information within the scope of the information sharing environment; and*
- *Replacing the standards described [above] with a standard that would allow mission-based or threat-based permission to access or share information (commonly known as an 'authorized use' standard) within scope of the ISE for a particular purpose determined to be lawfully permissible; and*
- *The use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the ISE in any cases in which: (1) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and (2) such use is consistent with any mission of that department, agency, or component that involves the storage, retention, sharing, or exchange of personally identifiable information.*[1]

1.2. Approach

This Report on the ISE presents the feasibility of the concepts that Congress has raised for consideration to promote information sharing. The Report addresses these issues by leveraging the expertise and knowledge of ongoing initiatives associated with these concepts across the Federal government. As such, the Report is organized in three distinct sections, each focused on one of the concepts based upon interagency efforts.

[1] *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act), P.L. 110-53, amending the *Intelligence Reform and Terrorism Prevention Act* (IRTPA Section 1016(j) (August 03, 2007).

2. Feasibility of Eliminating the Use of Markings that Restrict the Sharing of Information in the ISE

In the 9/11 Act, the Congress first requested the President to report on the feasibility of:

> *(A) eliminating the use of any marking or process (including `Originator Control') intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, between and among participants in the information sharing environment, unless the President has--`(i) specifically exempted categories of information from such elimination; and `(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph.*

2.1. The Current Environment

Although the elimination of unduly restrictive markings is essential to achieving information sharing and collaboration, it is also vital to national security that information be adequately protected and that appropriate controls are applied. Markings and processes that affect ISE information sharing are found in both unclassified (commonly referred to as "Sensitive but Unclassified") and classified information. A critical component of effective information sharing is a common understanding of, and standard for applying, control markings. Accordingly, the President and the departments and agencies participating in the ISE have taken steps to reduce, standardize and streamline the use, application, and impact of restrictive markings.

For example, SBU information is currently shared according to an ungoverned body of policies and practices. In 2005, the President directed that Sensitive But Unclassified (SBU) procedures for marking and handling terrorism-related information, homeland security information, and law enforcement information shared within the ISE be standardized.[2] The proposed recommendations to establish a framework that will rationalize SBU procedures are further detailed below (Section 2.2). In the classified realm, the inconsistent interpretation and application of Executive Order (EO) 12958[3] across the ISE impedes the sharing of classified information. The Intelligence Reform and Terrorism Prevention Act (IRTPA) directs that the Director of National Intelligence (DNI) shall, consistent with the protection of intelligence sources and methods from unauthorized disclosure, maximize the dissemination of intelligence by establishing and implementing guidelines for the Intelligence Community (IC). These guidelines are to provide direction to the IC on the (1) classification of information under Executive orders, Presidential directives or other applicable law; (2) access to and dissemination of intelligence; and (3) preparation of intelligence products in such a way that source

[2] Presidential Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment* (December 16, 2005).

[3] *Classified National Security Information,* Executive Order (EO) 12598 (as amended) (April 17, 1995).

information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.[4] As further detailed below (Section 2.3), the DNI has exercised this authority to issue policy direction to the IC to enhance information sharing. With specific respect to the application and use of the Originator Control or "ORCON" marking by IC elements, the Office of the Director of National Intelligence (ODNI) is currently evaluating the best solution for managing the goal of maximum interagency sharing of national security information with that of protecting the sources and methods on which the IC depends to gather such information.

2.2. Standardization of Procedures for Sensitive But Unclassified (SBU) Information

Current SBU sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism information that should be shared, but often fail to control the flow of information that should not be shared.[5] Because each department and agency largely establishes its own access controls, an individual who has access to controlled information in one agency may be denied access to that same information in another. Moreover, an organization that receives controlled information from several different Federal agencies often cannot be sure which controls should be applied to which markings from another agency. This greatly increases the likelihood of erroneous handling and dissemination of information. A control framework that is rational, standardized, and simplified will facilitate the sharing of ISE information that supports the individual missions of departments and agencies and enhances the ability to share vital terrorism information among Federal, State, local, tribal, and private sector entities, and foreign partners.

Presidential Guideline 3

On December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*. Specifically, Presidential Guideline 3 instructed that procedures and standards for designating, marking, and handling SBU information must be standardized across the Federal government.

The Guideline 3 Report

The proposed *Presidential Guideline 3 Report: Standardized Procedures for Sensitive But Unclassified Information* reflects an effort to comply with Presidential Guideline 3 requirements and recommends a new framework for rationalizing, standardizing, and simplifying procedures for SBU information in the ISE.

In response to this direction, a proposed Controlled Unclassified Information (CUI) Framework is under consideration. This framework would describe the mandatory policies and standards for designation, marking, safeguarding, and dissemination of all

[4] IRTPA, Section 102A(i)" to "Section 102A.(i) of the *National Security Act of 1947*, as amended by IRTPA.

[5] Across the Federal government there are more than 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information.

controlled unclassified terrorism-information, homeland security, and law enforcement information related to terrorism originated by the Federal government and shared within the ISE. Further, the framework would establish a simple marking schema that addresses both safeguarding and dissemination that will be used for all CUI. Two levels of safeguarding and dissemination standards will provide necessary protections for CUI, while facilitating its sharing in the ISE. However, there are certain important infrastructure protection agreements between the Federal Government and the Private Sector that are not fully accommodated under the proposed CUI framework due to additional safeguarding requirements. As a result, these federal regulations with their associated markings, safeguarding requirements, and dissemination limitations will be "grandfathered" into the CUI Framework.

An Executive Agent, in coordination with a CUI Council, will govern the new Framework and oversee its implementation. The CUI Executive Agent will develop and issue standards based on ISE-wide CUI policy.

2.3. Classification Standards and Processes to Promote Information Sharing

Significant efforts are being made by the DNI, in coordination with the PM-ISE, to standardize policies, processes and procedures for sharing classified information. These include key policy direction from the 500 Day Plan for Integration and Collaboration, creation of a Single Community Classification Guide[6] and related classification policy standards, and two Intelligence Community Policy Memorandums (ICPM 2007-200-2 & ICPM 2007-500-3), as well as efforts to rationalize the dissemination controls in the IC. The intent is to apply only those controls that are essential to protect intelligence sources and methods from unauthorized disclosure since inappropriate use can impede the efficient and timely access to intelligence information.

500 Day Plan for Integration and Collaboration

The DNI's "500 Day Plan for Integration and Collaboration" builds on the progress already achieved and more importantly, responds to today's new global environment. To ensure accountability, the ODNI established a Program Management Office to track, monitor and oversee execution of the 500 Day Plan and to report to senior leadership on a bi-weekly basis. This IC plan identifies six focus areas or priorities and delineates specific initiatives, within each focus area, to implement these priorities across the IC. The specific initiatives focus on those feasible actions for the IC that could demonstrate short-term progress and build momentum. The Focus Area, "Accelerate Information Sharing,"[7] concentrates on the improved collaboration needed to move from a philosophy of information ownership to one of information stewardship. To ensure that this seamless flow of information occurs among the different collection disciplines and analytic communities, the DNI is advancing this cultural shift from the pre-9/11 concept

[6] See also *Initiative 2D: Establish a Community Classification Guide, Focus Area 2: Accelerate Information Sharing* of the *500 Day Plan.*

[7] See *Focus Area 2: Accelerate Information Sharing* of the *500 Day Plan.*

of "need-to-know" toward a "responsibility to provide" mindset in order to better meet the current sharing needs consistent with the protection of sources and methods. As a member of the ISC, the ODNI works to increase IC coordination, collaboration, and alignment with similar activities across other Federal government communities.

Intelligence Community Policy Memorandums 2007-200-2 & 2007-500-3

Furthermore, the DNI has prioritized the "re-write [of] security policies and guidance in a way that, while protecting sensitive information, objectively weighs the risk of compromise against the risk to intelligence collection and analysis of not providing information to those who need it."[8] To this end, the DNI has recently promulgated two directives that promote information sharing and recognize the importance of protecting sources and methods, namely Intelligence Community Policy Memorandum (ICPM) 2007-200-2 and ICPM 2007-500-3.

ICPM 2007-200-2 provides that IC elements have the "Responsibility to Provide" intelligence information to all customers who require that information, consistent with law.[9] ICPM 2007-500-3 emphasizes the importance of this responsibility:

> *[t]he broadest possible sharing of intelligence information is fundamental to the mission of the IC. This responsibility, balanced by the obligations to protect national security information and the privacy and civil liberties of U.S. persons, is the guiding principle for all intelligence information sharing decisions.*[10]

In addition, ICPM 2007-500-3 stresses the notion that intelligence information is a "national asset" rather than something owned by an individual IC element and therefore directs that IC elements "implement policies, procedures, processes, and training needed to end the practice of intelligence information 'ownership' and implement the practice of intelligence information 'stewardship.'" As such, the IC elements are directed to "[p]rovide maximum access to and dissemination of intelligence information …while balancing the obligation of protecting intelligence sources and methods with the responsibility to provide intelligence information to meet customer mission requirements."

Dissemination Controls

Dissemination controls may unnecessarily inhibit information sharing within the ISE if the criteria for such controls are not specifically defined and if departments and agencies do not provide adequate training regarding their limited application. The current EO on classified national security information, EO 12958 (as amended by EO 13292)[11], sets forth standards for classifying, declassifying and safeguarding national security information. The EO provides that "[e]xcept as otherwise provided by statute, this order, directives implementing this order, or by direction of the President, classified

---

[8] Id.

[9] Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to meet the Intelligence Community's Responsibility to Provide*, released December 11, 2007.

[10] Intelligence Community Policy Memorandum (ICPM) 2007-500-3, *Intelligence Information Sharing*, released December 22, 2007.

[11] *Classified National Security Information*, EO 12598 (as amended) (April 17, 1995).

information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency." This provision, which has been referred to as the "third agency rule," requires an authorized recipient of classified information to obtain originator approval for the further dissemination of such information to a third agency. The concept of information "ownership" is reflected in, and reinforced by, this "third agency rule" and related Originator Controlled or "ORCON" markings, and must be addressed in light of the culture shift called for in the 500 Day Plan, which is necessary for the successful implementation of the ISE. Government personnel must serve as "stewards" of information rather than "information owners or holders" and must embrace their responsibility to provide information to those who need it to carry out their official duties.

The DNI's predecessor, the Director of Central Intelligence (DCI), provided initial relief from the "third agency rule", with application to the IC, in the Director of Central Intelligence Directive (DCID) 6/6 (DCID 6/6), which is still in effect today. This directive required IC elements to take a "risk management approach when preparing information for dissemination." They were instructed to "consider the needs of all appropriate intelligence consumers regarding sources and methods information or sensitive analytic comments" and use control markings only when necessary and in accordance with DCID 6/6. Moreover, IC elements were authorized to further disseminate classified information originating from within the IC to other executive branch departments and agencies without originator approval, unless such information was properly marked with an authorized control marking, such as "Not Releasable to Foreign Nationals (NOFORN)" or ORCON." These dissemination controls, listed as authorized markings in the Controlled Access Program Coordinating Office Register (CAPCO) [12], may only be applied to particularly sensitive classified information.

Modification of the third agency rule or the application of dissemination controls by elements outside the IC would be accomplished through presidential direction.

The DNI's Special Security Center has engaged ODNI stakeholders and the PM-ISE to discuss a new DNI dissemination control policy that will further refine the instances in which dissemination controls may be applied by the IC. The goal of this effort is a more integrated approach to the dissemination control policies, and as such, the initial focus of the discussions has been an improved understanding of ODNI stakeholders' perspectives on the future of dissemination controls. The imperative is to ensure that intelligence is provided to all who need it without delay or unnecessary restrictions. Through these discussions, the effort has identified key issues that will need to be addressed, to include: outdated dissemination controls criteria; the lack of accountability and oversight; and the lack of training and education. Resolution of these issues through the development and implementation of new ODNI policies will substantially

[12] The Controlled Access Program Coordination Office (CAPCO) was established under the authority of *Director of Central Intelligence Directive* (DCID) 3/29. The CAPCO maintains the Control Markings Register mandated by the revised DCID 1/7 and includes a list of authorized terms that may be used to mark classified materials and proscribes the exact format for their display. The CAPCO Register of *Authorized Controlled Markings and Implementation Manual* (October 12, 2000) creates a uniform method for marking classified information across the various government agencies.

improve information sharing by reducing the inconsistent application by IC agencies of dissemination controls. A revised dissemination control policy based on today's business practices and the "responsibility to provide" will also ensure alignment with related ODNI initiatives including the IC metadata standards and the IC classification guide currently under development.

3. Feasibility of Using 'Authorized Use' Standard in the ISE

The Congress also required the President to report on the following:

> *(B) continuing to use Federal agency standards in effect on such date of enactment for the collection, sharing, and access to information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;*
>
> *(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an `authorized use' standard).*

3.1. The Existing Framework – Sharing and Protecting under Current Standards

Federal agencies are required to follow certain rules, derived from applicable constitutional principles, laws, Executive Orders, regulations, and policies, regarding how they collect, retain, and disseminate certain information concerning U.S. persons. These include: the Privacy Act of 1974, as amended[13], the collection, retention and dissemination requirements set forth in EO 12333, as amended, and associated implementing procedures, as well as a myriad of other legal and policy requirements.

The Privacy Act limits how agencies can collect, retain, and disclose records about U.S. persons from a "system of records." In addition, EO 12333, as amended, provides that elements of the IC "are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General."[14] These rules – sometimes referred to as "U.S. Person rules" – are designed to protect privacy and civil liberties interests.

---

[13] 5 U.S.C. § 552a.

[14] EO 12333, *United States Intelligence Activities* (1981). EO 12333 defines a United States person "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."

These are merely examples of the rules and protections Federal agencies currently apply as they share terrorism information, homeland security information, and law enforcement information related to terrorism, in their development and use of the ISE. Other requirements derive from constitutional principles, applicable statutes (e.g., E Government Act of 2002, the Foreign Intelligence Surveillance Act, the Electronic Communications Privacy Act, the Right to Financial Privacy Act, etc.), and agency-specific regulations and policies. Application of these requirements is guided by agency offices of general counsel, and overseen and audited by agency offices of inspector general.[15] In addition, there is an increasing number of Federal privacy and civil liberties offices throughout the Federal government that have responsibilities relating to the implementation of these protections.[16] Congress has also established the Privacy and Civil Liberties Oversight Board, with government-wide responsibility to provide advice and oversight with respect to privacy and civil liberties matters relating to efforts to protect the Nation from terrorism, including those relating to the ISE.

ISE Privacy Guidelines

In mandating the creation of the ISE, Congress and the President recognized the need for privacy and civil liberties protections. Accordingly, guidelines were issued in November of 2006 - "Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment" ("ISE Privacy Guidelines"). The ISE Privacy Guidelines build on the Federal infrastructure currently in place, and provide the framework for enabling information sharing while protecting privacy and other legal rights. These guidelines call for agencies to comply with current laws, regulations, and policies related to information privacy and other legal rights, but they also require agencies to take pro-active and explicit actions to ensure that the balance between information privacy and security is maintained, building on a set of core principles that reflect basic privacy protections and best practices. They require internal agency policies and procedures, under a uniform government-wide framework, to identify and protect information about Americans that may be shared as part of the ISE, so that it is accessed, used, and retained consistent with authorized purposes and the need for information privacy and other legal protections.

---

[15] Other entities and offices may be involved as well, such as the Judge Advocate General's Corps for the uniformed branches in the Armed Services; the Assistant Secretary of Defense for Intelligence Oversight in the Department of Defense; compliance and inspection units within particular departments and agencies; etc.

[16] Certain departments have such positions established by statute, such as the Department of Homeland Security's (DHS) Privacy Office; DHS's Civil Rights and Civil Liberties Office; the Director of National Intelligence's (DNI) Civil Liberties and Privacy Office; the Department of Justice's (DOJ) Privacy and Civil Liberties Office; and privacy and civil liberties offices or positions established by the *9/11 Commission Act* at the Central Intelligence Agency and at the Departments of State, Treasury, Health and Human Services. In addition, the Office of Management and Budget (OMB) has directed that all agencies, regardless of statutory requirements, designate a senior official to be responsible for privacy matters. OMB has also established an interagency Privacy Committee consisting of those senior agency officials for privacy, co-chaired by OMB and DOJ, which meets regularly to discuss privacy matters of interagency concern.

Privacy Guidelines Committee

In addition, the ISE Privacy Guidelines establish a governance structure to provide ongoing guidance in the implementation of the guidelines and resolve issues as they arise. The ISE Privacy Guidelines Committee (PGC) is chaired by the ODNI's Civil Liberties Protection Officer and the Department of Justice's (DOJ) Chief Privacy and Civil Liberties Officer. It consists of the Privacy Officials of the departments and agencies of the ISC. This governance structure recognizes the difficulty of being able to predict in advance what information an agency will want to share, in what form, with what other entities, and under what circumstances, and therefore acknowledges that legal and policy protections cannot be predetermined for all sharing arrangements. Accordingly, the PGC has been developing additional guidance and implementation tools for agencies to use in determining how to facilitate the sharing of terrorism information while protecting privacy and other legal rights in accordance with the ISE Privacy Guidelines.

For example, the PGC recently authored the "Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment" to assist Federal agencies in implementing the guidelines. The guide translates elements of the guidelines into a process for agencies to follow to generate an ISE Privacy Protection Policy, as required by the ISE Privacy Guidelines that, in turn, is to be applied to the agency's ISE activities. The guide's dual-track "Identify/Assess/Protect" process model helps agencies focus on core privacy and civil liberties elements at the policy stage and at the information sharing stage to ensure that necessary protections are in place. At the end of this process, agencies will have identified and assessed the privacy and other legal requirements that apply to their information sharing arrangements, and put in place the protections needed to meet those requirements as well as the other requirements of the ISE Privacy Guidelines. The PM-ISE has recently published an online ISE Privacy Manual to provide additional guidance, including papers on key issues (redress, accountability/enforcement/audit, security, and notice mechanisms), research references, and background materials.[17]

An important function of the PGC is to serve as a forum for issues as they arise with respect to the implementation of the ISE Privacy Guidelines. In particular, we anticipate that as implementation continues, we will have the opportunity to address issues regarding personally identifiable information (PII), working with IC Offices of General Counsel, the Office of the ODNI, the DOJ, the Office of Management and Budget (OMB), the Department of Homeland Security, and other agencies and offices as appropriate. As stated in section 12 of the ISE Privacy Guidelines: "The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies."

---

[17] The ISE Privacy Guidelines, ISE Privacy Manual, and other ISE privacy information and resources, is available at: *http://www.ise.gov/pages/privacy-fed.html*

In that regard, it should be noted that the PGC[18] has representation from the members of the ISC, including OMB (which provides Privacy Act guidance to Federal agencies). Moreover, as a standing committee established by the PM-ISE, the PGC has ready access to the latest information regarding the development of the ISE.

This structure provides the PGC with direct access to not only the subject matter experts on privacy, civil liberties, and information sharing within the Federal government, but also to the offices and agencies with responsibility for issuing – and clarifying – guidance, interpretations, and policies with respect to U.S. person issues.

Implementation of the ISE Privacy Guidelines

The process for implementing the ISE Privacy Guidelines will serve as an important opportunity for each agency to identify, assess, and clarify the rules that apply to its own current sharing arrangements. The ISE Privacy Guidelines require that agencies implement an ongoing process to identify and assess the rules applicable to their sharing arrangements, and implement appropriate policies to ensure compliance with those rules. The Guidelines anticipate that as part of this process, agencies may encounter rules that may appear to serve no actual privacy-protective purpose. Section 2(c)(iii) of the ISE Privacy Guidelines establishes a process for escalating significant interagency impediments to information sharing to the PGC for review – this will help ensure that such interagency impediments are appropriately addressed by senior privacy officials, while necessary protections are preserved.

It is important to note that the PM-ISE is itself administratively placed within the ODNI, that the PGC is co-chaired by the ODNI's Civil Liberties Protection Officer, and that members of the IC (and the ISC), such as the Central Intelligence Agency, the National Counterterrorism Center (NCTC), and the Federal Bureau of Investigation, are participants in the PGC. In addition, the DNI recently established a formal interagency process (Intelligence Community Directive (ICD) 153) for reviewing and issuing interpretative guidance to the IC, in consultation with the ODNI's Civil Liberties Protection Officer, other privacy and civil liberties officials as appropriate, and in coordination with the DOJ, regarding procedures and guidelines governing the collection, retention, and dissemination of U.S. Person information under EO 12333. Thus, a mechanism now exists to achieve greater clarity and consistency in the application of US person principles across the IC.

Finally, although each of these new initiatives will enhance the protection of privacy and civil liberties while also advancing information sharing, it is important to note that information sharing is already taking place using processes and standards developed to protect privacy and civil liberties. For instance, NCTC has been established and has been fully operational for several years, and terrorist watch lists are being administered on a centralized basis by the Terrorist Screening Center. The dynamic sharing environment in which we currently operate involves, on a daily basis, the identification

[18] This includes representatives from the Departments of State (DOS); Transportation (DOT); Treasury; Interior; Health and Human Services (HHS); Energy (DOE); Commerce; and Defense (DoD)--which includes both Joint Chiefs of Staff and Office of the Secretary of Defense; DHS; DOJ; the Federal Bureau of Investigation (FBI); ODNI; OMB; the Central Intelligence Agency (CIA); the National Counterterrorism Center (NCTC); and the Program Manager for the Information Sharing Environment (PM-ISE).

and sharing of terrorism-related and the application of legal and policy requirements governing collection, retention, and dissemination activities.

3.2. Replacing the Current Standards with the "Authorized Use Standard"

The 9/11 Act requests an analysis of the feasibility of replacing the current "standards" with "a standard that would allow mission-based or threat-based permission to access or share information … for a particular purpose that the Federal Government, through an appropriate process … has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an `authorized use' standard)."

As discussed, the "standards" that are currently being followed are derived from existing constitutional principles, statutes, Executive Orders, and regulations, and have been put in place to protect privacy, legal and civil liberties interests. More work can and will be done to clarify those standards to make sure that agencies are operating with as consistent an understanding of common terms, definitions, and concepts as feasible given different missions, authorities, and functions.

Defining the "Authorized Use Standard"

The "authorized use standard" described in the 9/11 Act could be interpreted in different ways. One way to interpret it might be as follows: A regime operating under an "authorized use standard" would enable an appropriately credentialed official to access any information in the possession of a U.S. government agency based not on an application of legal and policy requirements currently in effect (the current "standards"), but rather on whether the official has the proper "mission-based or threat-based permission" to access that information. The key determination would be whether that permission was for a "lawful purpose," and the process for making that determination would be "established in consultation with the Privacy and Civil Liberties Oversight Board."

It is not clear whether this is the interpretation intended. If an official with the proper "mission- or threat-based permission" presented his or her credential to access any information about a person without regard to the Privacy Act, the Foreign Intelligence Surveillance Act, EO 12333, or any internal agency regulation or policy, information about individuals, and particularly, U.S. persons, would flow more freely. Privacy and civil liberties safeguards would need to be put in place to accommodate such a change, such as purpose and use limitations, disclosure limitations, and audit controls.

Such a regime would have significant privacy impacts as it could conflict with requirements in existing statutes, Executive Orders, and agency regulations. While some agency privacy protections are based on internal agency policies, many are implementations of the privacy and civil liberties protections required by Federal laws, Executive Orders, and regulations. Replacing existing standards with a uniform, government-wide "mission-based or threat-based" standard would, therefore, seem to require a "wipe-the-slate-clean" approach to privacy protection. It is not immediately apparent how such an approach would be feasible without, for example, legislation making clear that this "authorized use standard" supersedes any contravening privacy-

related laws or regulations. Since the 9/11 Act does not seem to contemplate that level of change in the privacy framework, we assume this is not the interpretation intended.

Markle Foundation Report: "Mobilizing Information to Prevent Terrorism"

In order to better understand the meaning of the "authorized use standard" referred to in paragraph (C), it is helpful to refer to the Third Report of the Markle Foundation Task Force, "Mobilizing Information to Prevent Terrorism" (Report).[19] The Report proposes adoption of "a new authorized use standard," and recommends guidelines to be applied across the government to support its implementation. While some statements in the Report might suggest that the authorized use standard calls for a wholesale replacement of existing rules, a closer reading reveals that the approach it recommends closely matches the one laid out in the ISE Privacy Guidelines and being followed in the ongoing work of the PGC.

In a section entitled "A New Authorized Use Standard," the Report discusses "Outdated distinctions for intelligence information."[20] It describes how "since the late 1970's, access to, and sharing of, lawfully-collected intelligence information between U.S. Government agencies has been controlled in significant measure by two factors: (1) whether such information was collected within the territory of the United States or overseas; and, (2) whether such information pertained to identified U.S. Persons (defined by law as U.S. citizens or permanent resident aliens)."[21] It explains how these distinctions are reflected in statute, Executive Orders, and agency guidelines, and how agencies have "adopted rules placing greater restrictions on sharing of information collected within the U.S. and on U.S. Persons than on other types of information."[22]

The Report then affirms the importance of these rules: "These rules were developed to protect U.S. Persons' civil liberties as guaranteed by the Constitution. The values they reflect must continue to be respected as the information sharing environment is implemented." Thus, the report acknowledges the existence and importance of the civil liberties protection infrastructure that already exists within the U.S. government.

The Report next turns to what it perceives to be significant problems with this system of protective rules. First, the Report points to "the impact of technology," noting that "[a]s much of the world's Internet traffic flows through the United States, and with new technical developments, it has become more difficult to determine whether information that has been lawfully collected relates to U.S. Persons, and sometimes even difficult to say where it is being collected."[23] Second, the Report states that "the government lacks clear, understandable, and consistently interpreted rules for access and sharing information that formerly was governed by the line at the border provided by where the

---

[19] The Third Report of the Markle Foundation Task Force, *Mobilizing Information to Prevent Terrorism* (henceforth referred to as, Markle Report) (July 2006), can be found at: http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf

[20] Markle Report, p. 32.

[21] Id.

[22] Id.

[23] Markle Report, p. 33.

information was collected or whether it was U.S. Persons information," and as a result, either too much or too little information may be getting shared.[24]

This leads the Report to recommend the adoption of the authorized use standard:

> *The government should replace the outdated rules governing information sharing and access for legally collected information with a new, coherent, and consistent regime based on an authorized use standard. An authorized use standard would improve the access, sharing, use, and protection of relevant information legally in the government's possession while protecting privacy and civil liberties.*
>
> *....*
>
> *Rules for information access and sharing should be based on the purpose for which the government party seeking access intends to use the information. An authorized use system, with such purpose clearly identified and approved in government-wide guidelines promulgated in advance and approved at the highest levels of government, should replace outdated rules based on the place of collection, U.S. Persons statutes, or other "line at the border distinctions."*
>
> *....*
>
> *As envisioned, an authorized use would be a mission- or threat-based justification to demonstrate that information was accessed or shared for a reason that the government, with public scrutiny, has determined beforehand to be appropriate and allowable.... Examples of an authorized use might include "Tracing of Terrorism-Related Financial Transactions;" "Responding to Threat to Civil Aviation in the Unites States;" and "Locating Known or Suspected Terrorists."*[25]

This should not be mistaken, however, as a call for new substantive laws relating to U.S. persons; rather, the Report makes clear that guidelines for implementing the authorized use standard "should be based on the legal authorities and specific mission of each agency, and reflect the sensitivity of the information and how the receiving official will use it, [and] must be consistent with the constitutional principles, statutes, Executive Orders, regulations, potential users' authorized mission, and that of their agency."[26] In addition, the Report states that the authorized use guidelines "would apply in particular, though not exclusively, to personally identifiable information about U.S. Persons. This kind of information will require especially careful handling."[27] And the Report acknowledges that the "authorized use articulation would not substitute for separate legal authority, where required, such as National Security letter or court order. If this additional authority is necessary under current law and regulation, then it should continue to be so."[28]

---

[24] Id.

[25] Markle Report, p. 34.

[26] Id.

[27] Markle Report, p. 35.

[28] Id.

Thus, authorized use guidelines should be developed in a way that:

- are based on the legal authorities of each agency,
- are based on the specific mission of each agency,
- reflect the sensitivity of the information,
- reflect how the receiving official will use the information,
- are consistent with constitutional principles,
- are consistent with statutes,
- are consistent with Executive orders,
- are consistent with regulations,
- are consistent with potential users' authorized mission,
- are consistent with the mission of the potential users' agency,
- apply in particular to U.S. Persons, and
- continue to require additional authority where required by law or regulation.

In order to be fully implemented, therefore, the authorized use standard necessarily calls for determinations that would take into consideration each of the factors listed above, a complex, agency-by-agency process involving reviews of agency missions and authorities, data sensitivities, and applicable rules (derived from law, Executive Orders, and regulations), based on the sharing being contemplated, and with particular focus on U.S. Person information.

The Report goes on to state that "legislation would set the framework for an authorized use regime and the Executive Branch would develop specific implementation through a formal high-level process with as much transparency as possible. This process would include the participating agency's ISE privacy and civil liberties officer, and should be reviewed by the Privacy and Civil Liberties Oversight Board prior to final approval by the President."[29] This does not appear to be a call for rewriting existing laws; rather, it envisions a "framework" for agencies to implement an authorized use standard.

ISE Privacy Guidelines

Read in this context, therefore, the authorized use standard and the guidelines to implement it, including the "framework" for doing so, look strikingly familiar. Indeed, strong parallels exist with the approach taken by the ISE Privacy Guidelines. The ISE Privacy Guidelines build on existing "standards" for protecting privacy and other legal rights of U.S. persons rather than calling for wholesale replacements of existing rules. They are government-wide guidelines issued within the existing legislative and Executive Branch framework. Like the authorized use standard, the ISE Privacy Guidelines involve careful agency-by-agency reviews and implementations, based on reviews of authorities and missions, and applicable laws and regulations, with particular emphasis on protecting U.S. person information.

The ISE Privacy Guidelines focus on establishing a common framework under which agencies take pro-active steps to identify their privacy protection responsibilities and information sharing arrangements, assess the adequacy of their existing policies and safeguards, and protect the information about U.S. persons being shared. At the end of

[29] Markle Report, p. 39.

that process, agencies will have an ISE Privacy Protection Policy that they apply to their information sharing arrangements. Once in place, this ISE Privacy Protection Policy would enable the agency to identify the information it can access and share, determine how it can be used, and ensure that the information is adequately protected.

A difference, of course, is that rather than being focused on driving uniform actions across Federal agencies to generate tailored privacy protection sharing policies, the authorized use standard focuses on establishing a "a mission- or threat-based justification to demonstrate that information was accessed or shared for a reason that the government, with public scrutiny, has determined beforehand to be appropriate and allowable." In this regard, it is important to note that to be "authorized," a use must be one that is covered by the legal authorities of the department or agency on whose behalf the person(s) would gain access to and use the information in question. Therefore, absent changes in existing law and policy, there cannot be established a "mission based" or "threat based" authority to access or use information that is independent of specific Agency authorities.

Nonetheless, the ISE Privacy Protection Policy can be viewed as, in part, performing a similar function to the authorized use standard. While not called an "authorized use standard," in practice, the policy will enable agencies to evaluate what they can – and cannot – access and share in their development and use of the ISE. In short, it informs agencies of their standard of "authorized use" from a privacy perspective.

It should be noted that some have commented about "myths," "misinterpretations," and "overinterpretations" of U.S. person rules, and that these have lead to cultural and systemic problems and risk aversion. While there is work that can – and is being – done to identify and clarify guidance and interpretations relating to such rules, it should also be noted that these are the same rules that, as recognized by the Markle Report, "were developed to protect U.S. Persons' civil liberties as guaranteed by the Constitution." As discussed, interagency processes have now been established to address U.S. person issues that arise in the context of sharing information within the ISE (e.g., the ICD 153 process, and the rules assessment process under the ISE Privacy Guidelines). In addition, the PGC will be considering additional tools and guides based on feedback received from agencies as work continues. If the concepts underlying the "authorized use standard" are helpful in addressing issues, they will be evaluated as part of those processes.

4. ISE Anonymization Feasibility

Lastly, the Congress requested the President to report on the feasibility of

> *(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which-- `(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and `(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information.*[30]

Data anonymization is the process of eliminating or obfuscating data so that the individual to whom the data pertains is not identifiable with reasonable efforts. Careful deployment of anonymization technology has the capacity to improve the privacy of US Persons in the context of the ISE, but raises feasibility issues that must be addressed.

It is important to note at the outset that different forms of data anonymization are already in use by agencies participating in the ISE. For example, intelligence community elements and law enforcement agencies use "minimization procedures" to minimize the collection, retention, and dissemination of information about U.S. persons, to satisfy requirements contained in statutes or agency guidelines.[31] Under such procedures, identifying information about a U.S. person is replaced with terms such as "US Person 1" and "Subject A."

Several issues must be addressed if agencies are to effectively implement and utilize technology that enables data anonymization capabilities across the ISE: (1) the maturity and effectiveness of commercially-available technologies are not fully understood in the context of a multi-Agency environment with multiple data formats and data-stores; (2) many operational systems and business processes were not designed to address anonymization and the application of anonymization technology to such systems and processes could, in some cases, reduce mission effectiveness; (3) systems and processes were designed to meet specific Agency mission requirements might be broader than those of the ISE; (4) possible need for re-identification of anonymized records in a multi-Agency environment; and (5) the integration of anonymization technology with other privacy controls.

---

[30] In this subsection, the definition of the term "anonymized data" is that provided by Congress in the 9/11 Act: "data in which the individual to whom the data pertains is not identifiable with reasonable efforts, including information that has been encrypted or hidden through the use of other technology." (as defined per the 9/11 Commission Act, Section 504(j)(2)).

[31] Such as the Foreign Intelligence Surveillance Act (FISA), Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 ("Wiretap Act"), and guidelines implementing EO 12333.

At this time, the research has not identified any single anonymization technique or product that will support anonymization throughout the ISE at this stage of development. Additionally, anonymization is just one approach from a suite of techniques for improving privacy. It should be feasible, however, to leverage anonymization technology, along with other privacy-enabling technologies, to provide agencies with an additional privacy tool. Of note, the best, most cost-effective results are realized by actively considering anonymization and other privacy-enabling technologies during the early stages of system and business process development. Retrofitting existing systems and processes to use anonymization is possible, but may entail significant costs or compromises. Science &Technology (S&T) organizations throughout the intelligence community are actively researching both existing products and potential technologies in pursuit of greater privacy protections that are compatible with mission effectiveness.

Maturity of Existing Technologies

Some anonymization capabilities are readily available in the form of commercial technologies. For example, a variety of tools exist that transform the contents of a database so as to de-identify them. However, the tools do not have the capacity to identify sensitive (e.g., PII) data automatically and rely on human experts to craft the rules that will be used to anonymize the data. This process may be time-consuming and can be fraught with error. For the ISE, this process would be further compounded by the decentralized nature of the ISE, as well as the variety of users and missions accessing and using anonymized data.

Furthermore, such tools usually work only with structured data, where the application of rules is more manageable. Unstructured data, such as free text, is much more difficult to process; yet, this is the form that many intelligence products take. It is worth noting that these tools can eliminate or obfuscate sensitive structured data in general, not just information directly or indirectly related to identity. Therefore, even in situations where de-identification is not feasible from a business process standpoint, such tools might still be capable of providing some measure of privacy protection.

Other, more sophisticated techniques for controlling the sharing of sensitive data exist, but it is not clear how resistant they are to circumvention. Sophisticated analytical techniques with expanded datasets available through the ISE may provide the opportunity, inadvertently or maliciously, to re-identify previously anonymized data. The ISE participants must have some level of trust or assurance that anonymization capabilities can resist such efforts. Therefore, careful consideration must be made when deciding how anonymized data is protected:

Should anonymized data retain the same protections as PII, if it was originally derived from PII?

Should all of the ISE participants adopt a single technology and set of anonymization rules?

Does the replication of data necessary to support most anonymization capabilities preclude their implementation from a resource perspective?

At this stage, extensive analysis of existing tools is required to determine the extent of their capabilities. Currently, S&T organizations are researching these tools and techniques to determine their effectiveness and suitability.

Existing Systems and Processes

Data anonymization (as well as other techniques) has the capacity to improve privacy while still enabling the use of potentially relevant information. However, inserting anonymization into existing systems and business processes that were not designed with anonymization in mind may impact mission effectiveness and prove cumbersome and costly. In addition to any technical or process modifications that may be required, implementation could necessitate time-consuming testing, re-certification and re-accreditation, and training. Deploying anonymization in these circumstances is feasible, but would require significant effort to retrofit existing systems and processes. Additionally, most anonymization technologies are designed for specific database formats and may not be interoperable with all of the technologies deployed by the ISE participants. The current systems containing sensitive data that require anonymization were designed to support a specific set of business processes during their systems planning and design phases. It is unclear whether overlaying anonymization capabilities would have a detrimental impact on existing consumer processes.

Privacy protections such as anonymization are best incorporated at the system planning and design stage because design and architecture decisions that do not take privacy controls into account can make it much more difficult to incorporate privacy protection later. Moreover, the requirements of sharing partners must be considered to ensure that controls are compatible with the needs of all stakeholders. Carefully considering appropriate privacy controls—including anonymization—at the earliest stages of the system development life cycle will save time and effort in the long run and help ensure that those controls have the desired effect.

Re-identification

One frequently overlooked issue is whether to deploy anonymization technology that is designed to allow the anonymization process to be reversed in order to re-identify the individual to whom information pertains. Associated with such a capability are questions that must be resolved regarding appropriate circumstances of use and safeguards against improper re-identification. In some situations, potential re-identification of data may be viewed as inappropriate, resulting in no provision for such a process. In other cases, the ability to re-identify information may be necessary to support data validation, further investigation, or some other purpose.

The ability to re-identify anonymized data is a spectrum rather than a binary property. The difficulty of re-identifying data, in those cases in which the capability has not been expressly provided, depends on a variety of factors. These include background knowledge that may support inferences and correlations that could lead to re-identification. The effort required to re-identify a given record is partially a function of the anonymization process, but it is also a function of the resources available to the entity attempting the re-identification. Therefore, the ultimate resistance of any record or data set to unauthorized re-identification is difficult to gauge. While some metrics have been

developed, estimating the adequacy of any given anonymization process can be problematic.

Some technologies are designed specifically to locate and allow re-identification of records of interest without revealing any other information. Such systems can potentially make the risk of unauthorized re-identification more ascertainable. Further evaluation of these products is necessary to assess both their utility and the strength of their protection schemes. Moreover, such tools are designed to support a very specific type of business process or objective.

Integration with Other Technologies

Even within the single area of anonymization, different technologies and approaches will vary in their applicability to any given ISE business process or objective. Anonymization alone, or any other type of privacy-enabling technology in isolation, cannot provide suitable privacy assurance across the entire ISE. Only a broad approach that systematically considers the characteristics of ISE business processes and aligns technologies with those processes will achieve the best possible level of privacy protection.

Anonymization technologies address one set of needs, but other technologies such as contextual access control and policy enforcement, data tagging and tracking, and more sophisticated auditing mechanisms—among others—are also necessary to support the privacy needs of the ISE. In implementing the ISE, government agencies will have to selectively deploy a variety of technologies to best enhance privacy while pursuing their missions.

5. Conclusion

As the Federal government responds to a new global environment, the imperative for effective information sharing has become and will remain a priority. The ***elimination of unduly restrictive markings*** is essential to achieving this information sharing and collaboration. However, for the ISE, this also means managing the need to share information vital to national security with that of protecting and applying appropriate restrictions to information that needs to be protected. Through IC-specific and broader ISE initiatives, the interagency is collaborating to achieve this dual imperative, to include: a common framework for Sensitive But Unclassified information; a framework of policies, processes, and procedures for sharing classified information; and a cultural shift from the concept of information "ownership" to one of information "stewardship."

An approach to establishing a uniform, government-wide ***authorized use standard*** for accessing and sharing U.S. Person information that is based on replacing existing rules with a "mission-based justification" would not be feasible because it would conflict with existing laws and protections. However, an authorized use standard that is based on agency missions and authorities, and based on constitutional principles and existing statutes, Executive Orders, and regulations - is generally consistent with the approach adopted by the ISE Privacy Guidelines, with the work currently being done by the PGC in providing guidance to implement those guidelines, and with the activities of Federal departments and agencies in their development and use of the ISE.

The deployment of ***anonymization technology*** has the capacity to improve the privacy of US Persons in the context of the ISE, but in the short term a single set of anonymization capabilities will not serve the needs of the missions supported by the ISE. The complexity and cost for the ubiquitous deployment anonymization capabilities across the ISE needs further study and tighter business process alignment.